Convolutional codes under linear systems point of view. Analysis of output-controllability

M. I. GARCÍA-PLANAS
Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada
Mineria 1, 08038 Barcelona
SPAIN
maria.isabel.garcia@upc.edu

El M. SOUIDI
Université Mohammed V
Département d'Informatique
B. P. 1014, Rabat
MOROCCO
emsouidi@yahoo.com

L.E. UM
Université Mohammed V
Département d'Informatique
B. P. 1014 , Rabat
MOROCCO
laurainlee@yahoo.fr

Abstract: In this work we make a detailed look at the algebraic structure of convolutional codes using techniques of linear systems theory. In particular we study the input-state-output representation of a convolutional code. We examine the output-controllability property and we give conditions for this property. At the end of the paper is presented a brief introduction to the analysis of output controllability for parallel concatenated codes.

Key–Words: Codes, linear systems, output-controllability.

1 Introduction

At the origin, coding theory has had mainly the fundamental dedication on information theory. In fact coding theory had arisen from the need for better communication and better computer data storage. Concretely convolutional codes are extensively used in many wireless transmissions systems such as transmitting information in deep space with remarkable clarity. These codes are oftentimes implemented in concatenation with a hard-decision code, particularly Reed Solomon. Before turbo codes, such constructions were the most efficient, coming closest to the Shannon limit.

The convolutional codes are binary codes that are an alternative to the block codes by their simplicity of generation with a little shift register. The convolutional codes were introduced by Elias [7] where it was suggested to use a polynomial matrix $G(z)$ in the encoding procedure and they allow to generate the code online without using a previous buffering.

Convolutional codes are used extensively in numerous applications as satellite communication, mobile communication, digital video, radio among others.

G. D Forney in [9] explained that the term "convolutional" is used because the output sequences can be regarded as the convolution of the input sequence with the sequences in the encoder.

A mathematical theory has been developed which has a strong relationship with algebra, combinatorics and algebraic geometry. Nowadays the coding theory is a very active area of research. There are many tasks related to the constructions of codes and relationships of coding theory with other areas of mathematics as linear algebra, linear systems theory for example.

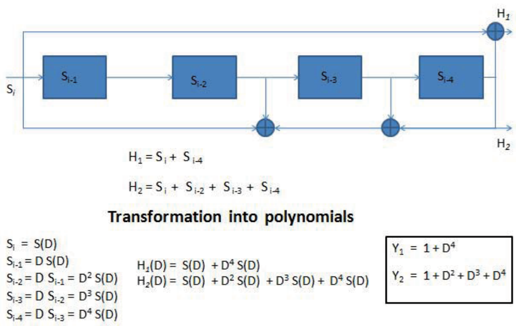
A key problem in convolutional codes theory was to find a method for constructing codes of a given rate and complexity with good free distance. Diverse methods have been introduced for this task. There is a considerable amount of literature on the theory of convolutional codes over finite fields, (see [7, 8, 13, 14, 16, 17, 19, 20, 23] for example).

A description of convolutional codes can be provided by a time-invariant discrete linear system called discrete-time state-space system in control theory (see [20, 22, 23]). We want to note that linear systems theory is quite general and it permits all kinds of time axes and signal spaces.

The aim of this article is to make a survey of the convolutional codes with the help of the tools of systems theory. Input-output representation of a convolutional code is examined, and output-controllable systems are characterized. The output controllability describes the ability of an external input to move the output from any initial condition to any final condition in a finite number of steps.

In the case of state space dynamical systems over real or complex numbers the the controllability and observability problem has been largely studied (see [5, 10, 11] for example). This problem for systems over commutative rings has also been studied (see [2, 18] for example). For convolutional codes theory, Rosenthal [21], presented a first step toward an algebraic decoding algorithm. It is based on an input/state/output description of the code and relies on the controllability matrix being the parity check matrix of an algebraically decodable block code. More recently other authors also study convolutional codes using the tools of control theory [3, 4, 15, 24], in particular in [3, 4], a characterization of some different models of concatenated convolutional codes from the perspective of linear systems theory is presented and also conditions so that the concatenated codes are observable are established.

The paper is organized as follows. In section 2 some basic notions about codes theory is introduced, in section 3 the definition of a convolutional code as linear system is given and the dynamic properties as output controllability are analyzed and a brief introduction to analysis of output controllable parallel convolutional codes is considered. Finally, in section 4 the conclusions are presented.



Convolutional code

2 Preliminaries

In this section, we present some basic notions about codes theory.

Let $\mathcal{A} = \{a_1, \cdots, a_q\}$ be a finite set of symbols, called alphabet of the message. We denote by $\mathcal{M}$ the set containing all sequences of symbols in $\mathcal{A}$ of length k. Also we denote by $\mathcal{R}$ the set consisting of all sequences of symbols in $\mathcal{A}$ of length n. We consider k and n positive integers with $k \leq n$.

We are interested in the case when $\mathcal{A} = \mathbb{F}_q = GF(q)$ the Galois field of q elements Z_q.

Consider $f : \mathcal{A} \longrightarrow \mathcal{A}^*$ where $\mathcal{A}^* = \bigcup_{n \geq 0} \mathcal{A}^n$ and $\mathcal{A}^n = \mathcal{A} \times \ldots \times \mathcal{A}$.

A code is defined as the image $f(\mathcal{A}^n) = \mathcal{C} \subseteq \mathcal{A}^*$.

We remark the following concepts:

- The left translation operator σ and the right translation operator σ^{-1} over the sequence spaces $\mathcal{A}^*$ are defined as: $\sigma(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots)$, $\sigma^{-1}(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots)$,
- $\mathcal{C} \subseteq \mathcal{A}^*$ is said to be invariant by right (left) translation when $\sigma^{-1}\mathcal{C} \subseteq \mathcal{C}$ ($\sigma\mathcal{C} \subseteq \mathcal{C}$).
- If for each element of $\mathcal{C}$ there is a finite number of non-zero elements, we say that $\mathcal{C}$ is compact.

Definition 1 *An error correcting code $\mathcal{C} \subseteq \mathcal{A}^*$ is said that is a convolutional code, when $\mathcal{C}$ is linear (considered as a vector space over $\mathbb{F}_q$ with the usual sum of vectors) invariant by right translation operator and has compact support.*

Following Rosenthal and York [22], a convolutional code is defined as a submodule of $\mathbb{F}^n[s]$.

Definition 2 *Let $\mathcal{C} \subseteq \mathcal{A}^*$ be a code. Then $\mathcal{C}$ is a convolutional code if and only if $\mathcal{C}$ is a $\mathbb{F}[s]$-submodule of $\mathbb{F}^n[s]$.*

Corollary 3 *There exists an injective morphism of modules*

$$\begin{aligned} \psi : \mathbb{F}^k[s] &\longrightarrow \mathbb{F}^n[s] \\ u(s) &\longrightarrow v(s). \end{aligned}$$

Equivalently, there exists a polynomial matrix $G(s)$ (called encoder) of order $n \times k$ and having maximal rank such that

$$\mathcal{C} = \{v(s) \mid \exists u(s) \in \mathbb{F}^k[s] : v(s) = G(s)u(s)\}.$$

The rate k/n is known as the ratio of a convolutional code. We denote by ν_i the maximum of all degrees of each of the polynomials of each line, we define the complexity of the encoder as $\delta = \sum_{i=1}^{n} \nu_i$, and finally we define the complexity convolution code $\delta(\mathcal{C})$ as the maximum of all degrees of the largest minors of $G(s)$.

The representation of a code by means a polynomial matrix is not unique, but we have the following proposition.

Proposition 4 *Two $n \times k$ rational encoders $G_1(s)$, $G_2(s)$ define the same convolutional code, if and only if there is a $k \times k$ unimodular matrix $U(s)$ such that $G_1(s)U(s) = G_2(s)$.*

After a suitable permutation of the rows, we can assume that the generator matrix $G(s)$ is of the form

$$G(s) = (P(s), Q(s))^T$$

with right coprime polynomial factors $P(s) \in \mathbb{F}^{(n-k)\times k}$ and $Q(s) \in \mathbb{F}^{k\times k}$, respectively.

3 Systems and Codes

A dynamic system is a model of an isolated fragment of the nature with a dynamic behavior that can be observed and studied: This behavior is the response of the system to an external stimulus, and this response may not be always the same, but rather depend also on the current circumstances of the dynamical system.

In other words, a dynamic system is a process which has a magnitude which varies with the time according a deterministic or stochastic law. More specifically:

Definition 5 *A dynamic system is a triple* $\Sigma = (T, \mathcal{A}, \mathcal{B})$ *where* $T \subseteq \mathbb{R}$ *is the time,* $\mathcal{A}$ *is the alphabet of signals, and* $\mathcal{B} \subseteq \mathcal{A}^T \subset \mathcal{A}^*$ *is the behavior. The elements of* $\mathcal{B}$ *are called trajectories.*

A linear model of a dynamical system can be represented in terms of variables depending on the times by the equations

$$\left.\begin{array}{rl} x_{t+1} & = Ax_t + Bu_t \\ y_t & = Cx_t + Du_t \end{array}\right\} \quad (1)$$

where $A \in M_\delta(\mathbb{F})$, $B \in M_{\delta\times k}(\mathbb{F})$, $C =\in M_{(n-k)\times\delta}(\mathbb{F})$ and $D \in M_{(n-k)\times k}(\mathbb{F})$. For simplicity and if confusion is not possible, we will write $p = n - k$. Also, we will write the system 1 simply as a quadruple of matrices (A, B, C, D).

3.1 Realization

From now on $T = Z^+$, $\mathcal{A} = \mathbb{F}^n$ where $\mathbb{F} = \mathbb{F}_q = GF(q)$ is a finite field (the q elements Galois field).

The proper rational matrix $P(s)Q(s)^{-1}$ is a coprime factorization of the transfer matrix of a dynamical system as (1).

Theorem 6 *Let* $\mathcal{C} \subseteq \mathbb{F}^n[s]$ *be un* k/n*-convolutional of complexity* δ*. Then, there exist matrices* K*,* L *of size* $(\delta+n-k)\times\delta$ *an a matrix* M *of size* $(\delta+n-k)\times n$ *having their coefficients in* $\mathbb{F}$ *such that the code* $\mathcal{C}$ *is defined as:*

$$\begin{array}{r} \mathcal{C} = \{v(s) \in \mathbb{F}[s] \mid \exists x(s) \in \mathbb{F}^\delta[s] : \\ sKx(s) + Lx(s) + Mv(s) = 0\} \end{array}$$

Moreover, K *is a column full rank matrix,* $\begin{pmatrix} K & M \end{pmatrix}$ *is a row full rank matrix and rang* $\begin{pmatrix} s_0K + L & M \end{pmatrix} = \delta + n - k$, $\forall s_0 \in \mathbb{F}$.

The triple (K, L, M) satisfying the above it is called *minimal representation* of $\mathcal{C}$.

Proposition 7 *If* (K_1, L_1, M_1) *is another representation of the convolutional code* $\mathcal{C}$*. Then, there exist invertible matrices* T *and* S *of adequate size, such that*

$$(K_1, L_1, M_1) = (TKS^{-1}, TLS^{-1}, TM). \quad (2)$$

Proof:

$$\begin{array}{r} \mathcal{C} = \{v(s) \in \mathbb{F}[s] \mid \exists x(s) = S^{-1}x_1(s) : \\ sK_1x_1(s) + L_1x_1(s) + M_1v(s) = 0\}. \end{array}$$

□

It is obvious that the relation (2) is an equivalence relation induced by the Lie group $\mathcal{G} = \{(T, S) \in Gl(\delta + n - k, \mathbb{F}) \times Gl(\delta; \mathbb{F})\}$.

Corollary 8 *The triple* (K, L, M) *can be written as:*

$$K = \begin{pmatrix} -I_\delta \\ 0 \end{pmatrix},\ L = \begin{pmatrix} A \\ C \end{pmatrix},\ M = \begin{pmatrix} 0 & B \\ -I_{n-k} & D \end{pmatrix}. \quad (3)$$

Proof: It suffices to make elementary row and column transformations to the matrix $\begin{pmatrix} K & L & M \end{pmatrix}$. □

As a corollary we have the following result.

Corollary 9

$$\begin{array}{r} \mathcal{C} = \{v(s) \in \mathbb{F}[s] \mid \exists x(s) \in \mathbb{F}^\delta[s] : \\ \begin{pmatrix} sI - A & 0 & -B \\ -C & I & -D \end{pmatrix} \begin{pmatrix} x(s) \\ v(s) \end{pmatrix} = 0\}. \end{array}$$

Proof: From theorem 6, we have

$$s\begin{pmatrix} I \\ 0 \end{pmatrix} x(s) - \begin{pmatrix} A \\ C \end{pmatrix} x(s) - \begin{pmatrix} 0 & B \\ -I & D \end{pmatrix} v(s) = 0,$$

and the result is obtained. □

If we divide the vector $v(s)$ into two parts $v(s) = (y(s), u(s))^T$ depending on the size of the matrix, the equality

$$\begin{pmatrix} sI - A & 0 & -B \\ -C & I & -D \end{pmatrix} \begin{pmatrix} x(s) \\ v(s) \end{pmatrix} = 0$$

can be expressed as

$$\left.\begin{array}{rl} sx(s) & = Ax(s) + Bu(s) \\ y(s) & = Cx(s) + Du(s) \end{array}\right\}.$$

Applying the Z antitransform we obtain the system

$$\left.\begin{array}{rl} x_{t+1} & = Ax_t + Bu_t \\ y_t & = Cx_t + Du_t \end{array}\right\} \quad (4)$$

Here $v_t = (y_t, u_t)^T$, $x_0 = 0$.

Remark 10 *We can obtain the encoder matrix* $G(z^{-1})$ *using the transfer matrix of the system (4).*

Example 1 Over $\mathbb{F} = Z_2$ we consider the following representation of a convolutional code

$$K = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix},\ L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix},\ M = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We have

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

And we obtain

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 1 \end{pmatrix}\ D = (1).$$

3.2 Convolutional code as input-state-output

Let $\mathbb{F} = \mathbb{F}_q$ be the q-elements Galois field and consider the matrices $A \in \mathbb{F}^{\delta\times\delta}$, $B \in \mathbb{F}^{\delta\times k}$, $C \in \mathbb{F}^{(n-k)\times\delta}$ and $D \in \mathbb{F}^{(n-k)\times k}$. A convolutional code $\mathcal{C}$ of rate k/n and complexity δ can be described by the following linear system of equations:

$$\left.\begin{aligned} x_{t+1} &= Ax_t + Bu_t \\ y_t &= Cx_t + Du_t \end{aligned}\right\},\quad v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix},\quad x_0 = 0. \tag{5}$$

In terms of systems theory the variable x_t is called a state variable of the system at time t, u_t the input vector and y_t the vector output obtained from the combination of input and state variable. If no confusion is possible, we will write the system as the quadruple of matrices (A, B, C, D).

Based on the system (5), one can find a minimal representation of a code, it suffices simply to define the triple (K, L, M) as (3).

In terms of the theory of codes, we have the input of the encoder after time t which is called the information o vector message u_t; the vector y_t created by the encoder is called parity vector, the code vector v_t is transmitted via the communication channel. We will denote the code convolution created in this way, by $\mathcal{C}(A, B, C, D)$.

In terms of the input-state-output representation of a convolutional code, the free distance of a convolutional code $\mathcal{C}$, that is, the minimum Hamming distances between any two code sequences of $\mathcal{C}$, can be characterized as (see [15])

$$d_{free}(\mathcal{C}) = \lim_{j\to\infty} d_j^c(\mathcal{C}), \tag{6}$$

where

$$d_j^c(\mathcal{C}) = \min_{u(0)\neq 0} \left\{ \sum_{t=0}^{j} wt(u(t)) + \sum_{t=0}^{j} wt(y(t)) \right\}$$

is the j-th column distance of the convolutional code $\mathcal{C}$, for $j = 0, 1, 2, \ldots$.

The free distance of a convolutional code determines to a large extend the error rate in the case of maximum likelihood decoding, and is a good indicator of the error correcting performance of the code.

It is well known that a manner to understand the properties of a dynamical system is treating it by purely algebraic techniques. The main aspect of this approach is defining an equivalence relation preserving the required properties, many interesting and useful equivalence relations between linear systems have been defined.

We want to define an equivalence relation over the set of quadruples (A, B, C, D) in such a way that the code representations (K, L, M), associated to the equivalent quadruples are equivalent under the equivalence relation defined in (2). Then we consider the following equivalence relation:

Definition 11 *The quadruple of matrices (A_1, B_1, C_1, D_1) is equivalent to (A, B, C, D) if and only if, there exist an invertible matrix $S \in Gl(\delta, \mathbb{F})$ such that:*

$$(A_1, B_1, C_1, D_1) = (SAS^{-1}, SB, CS^{-1}, D). \tag{7}$$

Obviously,

$$\left(\begin{pmatrix} -I_\delta \\ 0 \end{pmatrix}, \begin{pmatrix} A_1 \\ C_1 \end{pmatrix}, \begin{pmatrix} 0 & B_1 \\ -I_{n-k} & D_1 \end{pmatrix}\right) = (\mathcal{K}, \mathcal{L}, \mathcal{M})$$

with

$$\mathcal{K} = \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} -I_\delta \\ 0 \end{pmatrix} S^{-1},$$

$$\mathcal{L} = \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix} S^{-1},$$

$$\mathcal{M} = \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} 0 & B \\ -I_{n-k} & D \end{pmatrix}.$$

So, (K_1, L_1, M_1) is equivalent to (K, L, M).

We will note that the concept of minimality of an input-state-output representation is different from the concept of minimality of a representation, in classical linear systems theory. A representation (A, B, C, D) in linear systems literature is minimal if and only if the pair (A, B) is controllable and the pair (A, C) is observable. In fact, if the pair (A, B) is controllable, then the observability of the pair (A, C) ensures that the linear system (5) describes a noncatastrophic convolutional encoder, as we can see in the following lemma.

Lemma 12 (Lemma 2.11 of [22],) *Assume that the pair of matrices (A, B) is controllable. The convolutional code $C(A, B, C, D)$ defined through (5) represents an observable convolutional code if and only if the pair of matrices (A, C) is observable.*

Remember that a convolutional code is said catastrophic if it prone to catastrophic error propagation, i.e. a code in which a finite number of channel errors causes an infinite number of decoder errors. Any given convolutional code is or is not a catastrophic code.

3.3 Output-Controllability

One of the fundamental concepts in control theory is controllability. This is a qualitative property of the control systems and is of particular importance in control theory. The controllability systematic study began at the beginning of the sixties in the XX century and the study is based on the mathematical description of the dynamical system. In the literature there are many different definitions of controllability which depend on the type of dynamical system.

The most used definition of controllability is the state controllability requiring only that any initial state $x(0)$ can be steered to any final state x_1 with a finite number of steps. In this paper we will consider the output controllability that relates the input to the output, more concretely describes the control capability of input to the output.

Now we can try to solve the following problem: given $x(0) = 0$ and any $\bar{y}$ we can obtain a sequence of inputs $u(0), \dots, u(\delta)$ such that $y(k) = \bar{y}$. For that and in a more general form we consider the following definition.

Definition 13 *Dynamical system (5) is said to be output controllable if for every $y(0)$ and every vector $y_1 \in \mathbb{R}^p$, there exists a finite time t_1 and a control $u_1(t) \in \mathbb{R}^m$, that transfers the output from $y(0)$ to $y_1 = y(t_1)$.*

Therefore, output controllability generally means, that we can steer output of dynamical system independently of its state vector.

The existence of a solution of the problem is equivalent of the existence of the solution of the linear system equation $\bar{y} = CA^{\delta-1}Bu(0) + \dots + CABu(\delta - 2) + CBu(\delta - 1) + Du(\delta)$, that in a matrix form we have

$$\bar{y} = \begin{pmatrix} CA^{k-1}B & \dots & CAB & CB & D \end{pmatrix} \begin{pmatrix} u(0) \\ \vdots \\ u(k-2) \\ u(k-1) \\ u(k) \end{pmatrix}.$$

So, the existence of a solution is relied to the rank of the matrix of this system.

For a linear time-invariant system, like (5), described by matrices A, B, C, and D, we define the output controllability matrix

$$oC = \begin{pmatrix} CB & CAB & \dots & CA^{\delta-1}B & D \end{pmatrix}. \quad (8)$$

Remark 14 *Cayley-Hamilton theorem ensures that the range of the matrix*

$$\begin{bmatrix} CB & CAB & \dots & CA^{\delta-1}B & D \end{bmatrix}$$

coincides with the range of the matrices

$$\begin{bmatrix} CB & CAB & \dots & CA^{i}B & D \end{bmatrix} \ \forall i \geq \delta.$$

We have the following result.

Theorem 15 *Dynamical system (5) is output controllable if and only if the matrix oC has full row rank:* rank $oC = p$.

Example 2 The system associated with the code in Example 1 is output controllable:

$$\text{rank} \begin{pmatrix} CB & CAB & D \end{pmatrix} = \text{rank} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} = 1$$

Remark 16 *As we said at the beginning of this subsection, another important property and largely studied is the state controllability characterized by the rank of the controllability matrix*

$$\mathcal{C} = \begin{pmatrix} B & AB & \dots & A^{\delta-1}B \end{pmatrix}$$

in the sense that the dynamical system (5) is controllable if and only if the matrix $\mathcal{C}$ has full row rank. Like in the case of output controllability we observe that the range of the matrix

$$\begin{bmatrix} B & AB & \dots & A^{\delta-1}B \end{bmatrix}$$

coincides with the range of the matrices

$$\begin{bmatrix} B & AB & \dots & A^{i}B \end{bmatrix}, \forall i \geq \delta.$$

It should be pointed out, that the state controllability is defined only for the linear state equation, whereas the output controllability is defined for the input-output description i.e., it depends also on the linear algebraic output equation. Therefore, these two concepts are not necessarily related.

The following example shows that the concepts of output-controllability and controllability are not equivalent.

Example 3 a) Consider the system (A, B, C, D) with

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

and

$$C = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \ D = (0).$$

Clearly,

$$\operatorname{rank} \begin{pmatrix} CB & CAB & CA^2B \end{pmatrix} = 1$$

so, the system is output-controllable. And

$$\operatorname{rank} \begin{pmatrix} B & AB & A^2B \end{pmatrix} = 2 < 3,$$

so, the system is not controllable

b) Suppose now the system (A, B, C, D) with

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \ D = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Clearly,

$$\operatorname{rank} \begin{pmatrix} CB & CAB \end{pmatrix} = 1 < 2,$$

so, the system is not output controllable. And

$$\operatorname{rank} \begin{pmatrix} B & AB \end{pmatrix} = 2$$

So, the system is controllable.

c) There may be systems that simultaneously are controllable and output-observable as for example the system (A, B, C, D) with

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \ D = (0).$$

Clearly

$$\operatorname{rank} \begin{pmatrix} CB & CAB & CA^2B \end{pmatrix} = 1,$$

so, the system is output controllable. And

$$\operatorname{rank} \begin{pmatrix} B & AB & A^2B \end{pmatrix} = 3$$

so, the system is controllable.

d) And finally we also present a system that is neither output controllable nor controllable as for example the system (A, B, C, D) with

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \ D = (0).$$

Clearly,

$$\operatorname{rank} \begin{pmatrix} CB & CAB & CA^2B \end{pmatrix} = 0 < 1,$$

so, the system is not output controllable. And

$$\operatorname{rank} \begin{pmatrix} B & AB & A^2B \end{pmatrix} = 1 < 3,$$

so, the system is not controllable.

Proposition 17 *The output controllability character is invariant under feedback.*

Proof: Let $F \in M_{k\times\delta}(\mathbb{F})$ be a feedback, then the system under feedback is

$$(A + BF, B, C + DF, D).$$

Now, it suffices to compute the submatrices $(C + DF)(A + BF)^iB$ constituting the output-controllability matrix.

$$\begin{array}{l} (C+DF)(A+BF)^iB = \\ CA^iB + \sum_{0\leq\ell\leq i-1} CA^{i-\ell-1}BF(A+BF)^\ell B + \\ DFA^iB + \sum_{0\leq\ell\leq i-1} DFA^{i-\ell-1}BF(A+BF)^\ell B. \end{array}$$

In the case where $D = 0$ a proof can be found in [6]. □

Remark 18 *We observe that if the matrix C is the identity matrix this result ensures that the state controllability is also invariant under feedback.*

The above proposition induces to consider the following equivalence relation

Definition 19 *The dynamical systems (A_i, B_i, C_i, D_i), $i = 1,2$ are equivalent if and only if, there exist matrices $S \in Gl(\delta; \mathbb{F})$, $R \in Gl(m; \mathbb{F})$, $T \in Gl(q; \mathbb{F})$, $F \in M_{m\times\delta}(\mathbb{F})$ such that $A_2 = SA_1S^{-1} + SB_1F$, $B_2 = SB_1R$, $C_2 = TC_1S + TD_1F$, $D_2 = TD_1R$.*

It is immediate that if we take the subset formed by $R = I, T = I, F = 0$ we obtain the relation (7).

Proposition 20 *The output controllability is invariant under the new equivalence relation.*

Proof: Taking into account proposition 17, it suffices to prove that the output controllability is invariant under basis change in the state, input and output spaces.

Let (A_1, B_1, C_1, D_1) be a quadruple equivalent to (A, B, C, D) under basis change in the state input and output spaces, that is

$$(A_1, B_1, C_1, D_1) = (SAS^{-1}, SBR, TCS, TDR).$$

We observe that

$$C_1A_1^iB_1 = TCSS^{-1}A^iS^{-1}SBR = TCA^iBR.$$

So,

$$\begin{array}{l}\operatorname{rank}\begin{pmatrix} C_1B_1 & C_1A_1B_1 & \dots & C_1A_1^iB_1 & D_1\end{pmatrix}\\ \operatorname{rank} T\begin{pmatrix} CB & CAB & \dots & CA^iB & D\end{pmatrix}R\end{array}$$

□

Proposition 21 *Let (A_i, B_i, C_i, D_i), $i = 1,2$ be two equivalent dynamical systems. Then*

$$\operatorname{rank}\begin{pmatrix} C_1 & D_1\end{pmatrix} = \operatorname{rank}\begin{pmatrix} C_2 & D_2\end{pmatrix}.$$

Proof: If (A_i, B_i, C_i, D_i), $i = 1,2$ are equivalent, following the definition 19 there exist matrices $S \in Gl(\delta; \mathbb{F})$, $R \in Gl(m; \mathbb{F})$, $T \in Gl(q; \mathbb{F})$, $F \in M_{m\times\delta}(\mathbb{F})$ such that $A_2 = SA_1S^{-1} + SB_1F$, $B_2 = SB_1R$, $C_2 = TC_1S + TD_1F$, $D_2 = TD_1R$. So,

$$\begin{array}{l}\operatorname{rank}\begin{pmatrix} C_1 & D_1\end{pmatrix} = \\ \operatorname{rank} T\begin{pmatrix} C_1 & D_1\end{pmatrix}\begin{pmatrix} S^{-1} & \\ F & R\end{pmatrix} = \\ \operatorname{rank}\begin{pmatrix} C_2 & D_2\end{pmatrix}.\end{array}$$

In order to obtain conditions for output-controllability we consider an equivalent quadruple (A_c, B_c, C_c, D_c) with $D_c = \begin{pmatrix} 0 & 0 \\ 0 & I_d\end{pmatrix}$, $d = \operatorname{rank} D$,

$B_c = \begin{pmatrix} B_1 & 0, \end{pmatrix}$,

$(A_c, B_1) = \left(\begin{pmatrix} N & \\ & J\end{pmatrix}, \begin{pmatrix} B_{11} \\ 0\end{pmatrix}\right)$ is a pair of matrices in its Kronecker reduced form and

$C_c = \begin{pmatrix} C_{11} & C_{12} \\ 0 & 0\end{pmatrix}$,

all blocks in matrices are of adequate size. (For more information about canonical reduced forms see [12]).

Taking into account proposition 21 and the reduced form we can consider triples of matrices (A, B, C) and announce the main result.

Theorem 22 *Let (A, B, C) be a triple of matrices in its reduced form. Then*

i) If $p > \delta$ the system is not output-controllable,

ii) If $p \leq \delta$ the system is output-controllable if and only if $\operatorname{rank} C_{11} = p$.

Proof: Let $k_1 \leq \ldots \leq k_r$ the Kronecker indices of (A, B).

Observe that $C_{11} \in M_{p\times k_1+\ldots+k_r}(\mathbb{F})$.

$$\begin{array}{l}\operatorname{rank}\begin{pmatrix} CB & CAB & \dots & CA^{n-1}B\end{pmatrix} = \\ C_{11}\begin{pmatrix} B_{11} & NB_{11} & \dots & N^{k_r}B_{11}\end{pmatrix}.\end{array}$$

Matrix $\begin{pmatrix} B_{11} & NB_{11} & \dots N^{k_r}B_{11}\end{pmatrix}$ has full rank equal to $\sum_{i=1}^{k_r} k_i$. □

In the particular case where (A, B) is completely controllable we have the following corollary.

Corollary 23 *Let (A, B, C) be a triple of matrices such that the pair (A, B) is controllable, Then the system is output controllable if and only if*

$$\operatorname{rank} C = p \leq \delta$$

Example 4 Let (A, B, C) be a triple with

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0\end{pmatrix},$$

$$B = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0\end{pmatrix}$$

and

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{p1} & c_{p2} & c_{p3} & c_{p4} & c_{p5} \end{pmatrix}.$$

Following theorem the system is output controllable if and only if rank $C = p$ and it is not possible if $p > 5$.

In this case is easy to compute the output controllability matrix and obtain the rank:

$$\text{rank} \begin{pmatrix} oC_1 & oC_2 & oC_3 \end{pmatrix} = r,$$

where

$$oC_1 = \text{rank} \begin{pmatrix} c_{13} & c_{15} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ c_{p3} & c_{p5} & 0 & \dots & 0 \end{pmatrix},$$

$$oC_2 = \text{rank} \begin{pmatrix} c_{12} & c_{14} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ c_{p2} & c_{p4} & 0 & \dots & 0 \end{pmatrix},$$

$$oC_3 = \text{rank} \begin{pmatrix} c_{11} & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ c_{p1} & 0 & 0 & \dots & 0 \end{pmatrix}.$$

So

$$r = \text{rank} \begin{pmatrix} c_{13} & c_{15} & c_{12} & c_{14} & c_{11} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{p3} & c_{p5} & c_{p2} & c_{p4} & c_{p1} \end{pmatrix} = \text{rank}\, C.$$

3.3.1 Parallel concatenated codes

In coding theory, concatenated codes form a class of error-correcting codes that are derived by combining an inner code and an outer code. They were conceived in 1966 by Dave Forney as a solution to the problem of finding a code that has both exponentially decreasing error probability with increasing block length and polynomial-time decoding complexity.

Consider now two convolutional codes $\mathcal{C}_1(A_1, B_1, C_1, D_1)$ and $\mathcal{C}_2(A_2, B_2, C_2, D_2)$. Let $x_1(t)$, $u_1(t)$, and $y^{(1)}(t)$ be the state vector, the information vector and the parity vector of $\mathcal{C}_1(A_1, B_1, C_1, D_1)$, and let $x_2(t)$, $u_2(t)$, and $y_2(t)$ be the state vector, the information vector and the parity vector of $\mathcal{C}_2(A_2, B_2, C_2, D_2)$, respectively.

Suppose that both codes are concatenated in a parallel form, so that the input information $u_2(t) = u_1(t) = u(t)$ and the final parity vector $y(t) = y_1(t) + y_2(t)$.

Consequently,

$$\begin{aligned} x_1 &= A_1 x_1(t) + B_1 u(t) \\ x_2 &= A_2 x_2(t) + B_2 u(t) \\ y(t) &= C_1 x_1(t) + C_2 x_2(t) + (D_1 + D_2) u(t). \end{aligned}$$

That in a matrix form we have

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},\ B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$$
$$C = \begin{pmatrix} C_1 & C_2 \end{pmatrix},\ D = D_1 + D_2.$$

If $\mathcal{C}_1(A_1, B_1, C_1, D_1)$ is a (n, k, δ_1)-code and $\mathcal{C}_2(A_2, B_2, C_2, D_2)$ is a (n, k, δ_2)-code, then $\mathcal{C}(A, B, C, D)$ is a $(n, k, \delta_1 + \delta_2)$-code.

The transfer matrix of the concatenated system can be deduced directly from the transfer matrices of the initial systems.

Proposition 24

$$C(zI_{\delta_1+\delta_2} - A)^{-1}B = C_1(zI_{\delta_1} - A_1)^{-1}B_1 + D_1 + C_2(zI_{\delta_2} - A_2)^{-1}B_2 + D_2.$$

For more information about concatenated codes see [1], for example. The output controllability of the codes does not ensure the output controllability of the concatenated code as we can observe in the following example.

Example 5 Consider the following systems in Z_2,

$$A_1 = A_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ B_1 = B_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$C_1 = C_2 = \begin{pmatrix} 1 & 0 \end{pmatrix},\ D_1 = D_2 = (1).$$

The concatenated system is

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix},\ D = (0).$$

It is obvious that the systems (A_i, B_i, C_i, D_i) are output controllable. But the output controllable matrix is the zero matrix.

In fact the output controllability of the systems is not a necessary condition.

Example 6 Consider the following systems in Z_2,

$$A_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ B_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 0 \end{pmatrix},\ D_1 = (1),$$

and

$$A_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ B_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 0 & 1 \end{pmatrix},\ D_2 = (1).$$

The concatenated system is

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix},\ D = (0).$$

The system (A_2, B_2, C_2, D_2) is not output controllable but the concatenated system is output controllable.

Therefore, there is not a direct relation between output controllability of the systems and the output controllability of the concatenated system. But, some sufficient conditions can be obtained.

Proposition 25 *A sufficient condition for the output controllability of concatenated system is*

$$\operatorname{rank}(D_1 + D_2) = p.$$

Example 7 Consider the following systems in Z_2

$$A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$C_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ D_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

and

$$A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ B_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$C_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ D_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

Clearly,

$$\operatorname{rank}(D_1 + D_2) = 2.$$

Then, the concatenated parallel system is output controllable.

4 Conclusions

In this paper a detailed look at the algebraic structure of convolutional codes using techniques of linear systems theory has been made. In particular a study of the input-state-output representation of a convolutional code has been presented. The output-controllability property has been introduced and conditions for this property have been given. Finally, a brief introduction to analysis of output controllability for parallel concatenated codes is given.

Acknowledgements: This work has been supported by AECID "Agencia Española de Cooperación Internacional para el Desarrollo" within the framework of the Inter-University Research Cooperation between Spain and the Mediterranean Countries under the Grant A/030070/10.

References:

[1] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, Parallel concatenated trellis coded modulation, in *Proc. IEEE Int. Conf. Communications*, vol.2, Dallas, TX, June 1996, pp. 974-978.

[2] M. Carriegos, *Equivalencia Feedback en Sistemas Dinámicos lineales*, Tesis Doctoral, Valladolid, España, (1999).

[3] J-J. Climent, V. Herranz, C. Perea, A first approximation of concatenated convolutional codes from linear systems theory viewpoint, *Linear Algebra and its Applications*, vol.425, (2007), pp. 673-699.

[4] J-J. Climent, V. Herranz, C. Perea, Linear system modelization of concatenated block and convolutional codes, *Linear Algebra and its Applications*, vol.429, (2008), pp. 1191-1212.

[5] A. Díaz, M. I. García-Planas, An alternative collection of structural invariants for matrix pencils under strict equivalence, *Wseas Transactions on Systems and Control*, vol.10,(2009), 4: pp 487-496.

[6] J. L. Dominguez-García, M. I. García-Planas, Output controllability analysis of fixed speed wind. To appear in *IPACS electronic library*, (2011).

[7] P. Elias, Coding for Noisy Channels, *IRE Conv.Rec.*, vol.4, (1955), pp. 37-46.

[8] Ch. Fragouli, R. D. Wesel, Convolutional Codes and Matrix Control Theory, *Proceedings of the 7th International Conference on Advances in Communications and Control*, Athens, Greece, (1999).

[9] G. D. Forney, Convolutional codes: Algebraic structure, *IEEE trans. Information Theory*, (1970).

[10] M. I. García-Planas, Sensivity and stability of singular systems under proportional and derivative feedback, *Wseas Transactions on Mathematics*, vol.8, (2009), 11: pp 635-644.

[11] M. I. García-Planas, Bifurcation diagrams of generic families of singular systems under proportional and derivative feedback, *Wseas Transactions on Mathematics*, vol.7,(2008), 2: pp. 1-11.

[12] M. I. García-Planas, M. D. Magret, An alternative System of Structural Invariants for Quadruples of Matrices, *Linear Algebra and its Applications*, vol.291,(1999), (1-3), pp. 83-102.

[13] H. Gluesing-Luerssen., U. Helmke, J.I. Iglesias Curto Algebraic Decoding for Doubly Cyclic Convolutional Codes, *Advances in Mathematics of Communications*, vol.4,(2010), pp.83-99

[14] Heide Gluesing-Luerssen, G. Schneider, State space realizations and monomial equivalence for convolutional codes, *Linear Algebra and its Applications*, vol.425, (2007), 518-533.

[15] R. Hutchinson, J. Rosenthal, R. Smarandache, Convolutional codes with maximum distance profile, *Systems Control Lett.*, vol.54, (2005), 1: pp- 53-63.

[16] J. I. Iglesias, *A study on convolutional Codes, Classification, new families and decoding*, Tesis Doctoral, (2007).

[17] M. Kuijper, R. Pinto, On minimality of convolutional ring encoders, *IEEE Trans. on Information Theory*, vol.55, (2009), 11: pp. 4890-4897.

[18] H. Loeliger, G. D. Forney, T. Mittelholzer, M.D. Trot, Minimality and observability of group systems, *Linear Algebra and its Applications*, vol.205-206,(1994), pp. 937-963.

[19] J. L. Massey, M. K. Sain, Codes, Automata and continuous systems: explicit interconnections, *IEEE Trans. on Automatic Control*, vol.AC-12, (6),(1967), pp.644-650.

[20] J. Rosenthal, Some interesting problems in systems theory wich are of fundamental importance in coding theory, *Proceedings of the 36th IEEE Conference on Decision and Control*, (1997).

[21] J. Rosenthal, An algebraic decoding algorithm for convolutional codes, In G. Picci and D. S. Gilliam, editors, *Dynamical Systems, Control, Coding, Computer Vision; New Trends, Interfaces, and Interplay*, pp. 343-360. Birkhäuser, Basel, (1999).

[22] J. Rosenthal, E. V. York, BCH Convolutional Codes, *IEEE Trans. Information Theory*, vol. 45, (1999),6: pp. 1833-1844, .

[23] J. Rosenthal, J. M. Schumacher, E. V. York, On Behaviors and Convolutional Codes, *IEEE Trans. on Information Theory*, vol.42, (1996), (6): pp. 1881-1891.

[24] E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, *Asian Journal of Control*, vol.12,(2010), 2: pp. 119-126.